Implementing strong user authentication with Windows Hello for Business

In Windows 10, the Windows Hello for Business (formerly known as Microsoft Passport for Work) feature can replace passwords with strong two-factor authentication that combines an enrolled device with a PIN or biometric (fingerprint or facial recognition) user input to sign in. With the Windows 10 Anniversary Update, Core Services Engineering and Operations (CSEO, formerly Microsoft IT) streamlined the deployment of this feature as an enterprise credential to improve the user sign-in experience and to increase the security of accessing corporate resources.

Using this feature, users can authenticate to a Microsoft account, an Active Directory account, or a Microsoft Azure Active Directory (Azure AD) Premium account.

The Windows Hello for Business feature is a public key or certificate-based authentication approach that goes beyond passwords. This form of authentication relies on key pairs that can replace passwords and are resistant to breaches, thefts, and phishing.

Other benefits of this feature include:

- **It supports our Zero Trust security model.** Emphasizes an identity-driven security solution by centering on securing user identity with strong authentication as well as eliminating passwords.
- **It uses existing infrastructure.** We configured Windows Hello to support smart card–like scenarios by using a certificate-based deployment. Our security policies already enforced secure access to corporate resources with two-factor authentication, including smart cards and Microsoft Azure Multi-Factor Authentication. Windows Hello is currently enabled, and we anticipate an increase in usage as more biometric-capable devices become available in the market.
- **It uses a PIN.** Replace passwords with a stronger authentication. Users can now sign in to a device using a PIN that could be backed by a trusted platform module (TPM) chip.
- **It provides easy certificate renewal.** Certificate renewals automatically occur when a user signs in with their PIN before the lifetime threshold is reached.
- **It permits single sign on.** After a user signs in with their PIN, the user has access to email, SharePoint sites, when using the latest Office 365 versions, and business applications without being asked for credentials again.
- **It is compatible with remote access.** When using a certificate-based PIN, users can connect remotely using a CSEO VPN without the need for multi-factor authentication with phone verification.
- **It supports Windows Hello.** If users have compatible biometric hardware, they can set up biometrics sign-in to swipe their finger or take a quick look at the device camera.

Our deployment environment for the Windows Hello for Business feature include:

- **Server.** Azure AD subscription and Azure AD Connect to extend on-premises directory to Azure AD:
  - For certificate-based: Active Directory Certificate Services (AD CS), Active Directory Federation Services (AD FS) Network Device Enrollment Service (NDES), and Microsoft Intune
- **Client.** A device, preferably with an initialized and owned TPM, running Windows 10 Anniversary Update.

For more information about integrating on-premises identities with Azure AD, see [Integrating your on-premises identities with Azure Active Directory](#).

**Enrollment and setup**

Windows Hello for Business user enrollment steps vary, based on our deployed scenarios. For all scenarios, users will need to use their smart card or multi-factor authentication with a verification option—such as a phone call or verification on a mobile app, such as **Microsoft Authenticator**, in addition to their user name and password—to complete the enrollment.
The Windows Hello for Business feature supports the following enrollment scenarios:

- **On-premises Active Directory domain-joined devices.** Users sign in with their domain account, the Group Policy is applied, the device is registered with Azure Active Directory, and then the user creates a PIN.

- **Azure AD-joined devices managed by Microsoft Intune.** Users must enroll in device management (or add a work account) through Microsoft Intune. After their device is enrolled and the policies are applied, the PIN credential provisioning process begins and users receive the prompt to create their PIN.

### Requirements

- Two-factor authentication is required for PIN creation using one of the existing methods (virtual smart card, physical smart card, or multi-factor authentication with phone verification).
- A PIN that is at least six characters long.
- A connection to the internet or Microsoft corporate network.

### Physical architecture

Our Windows 10 domain-joined devices were already synchronized with Azure AD through Azure AD Connect, and we already had a public key infrastructure (PKI) in place. Already having PKI reduced the amount of change required in our environment to enable the Windows Hello for Business feature.

To deploy user certificates based on Windows Hello keys, we used AD FS, AD CS, and Group Policy.

---

*Figure 1. Windows Hello for Business architecture*
Server roles and services
In our implementation, the following servers and roles work together to enable Windows Hello as a corporate credential:

- Azure AD subscription with Azure Active Directory Device Registration Service to register devices with Azure Active Directory.
- Microsoft Intune is used to enroll devices joined to Azure Active Directory.
- AD FS is used for federated identities and Azure AD Application Proxy for secure remote access of web applications hosted on-premises. AD FS Registration Authority is used to handle certificate issuances and renewals for devices that are joined to the domain.
- PKI includes NDES servers (with policy module) and certificate authorities (with smart card EKU—enhanced key usage—template), used for the issuance, renewal, and revocation of Windows Hello for Business certificates.

Domain-joined service workflow
The following workflow applies to any Windows 10 computers joined to our AD DS domain.

- Our domain-joined Windows 10 devices pull a Group Policy object that configures certificate enrollment, PIN-enablement, and notification tasks.
- After users sign out and sign in again, or if they select the pop-up notification when it displays, a PIN creation workflow runs, and they must configure their new PIN.
- During the next sign-in, the user is prompted to configure Windows Hello for Business, confirm their identity using multifactor authentication, and create a PIN. A private key is created and registered in Azure AD. The user can also initiate the Windows Hello setup process from the Settings app at any time.
  - If the client and infrastructure support Instant-On, a key-receipt verification package is downloaded and a certificate request is sent to the AD FS registration authority. AD FS confirms valid key ownership and submits the request on behalf of the user to an AD CS certification authority.
- The certificate is delivered to the computer.

Azure Active Directory–joined service workflow

- Windows Intune pushes a device policy to Azure Active Directory devices that contains the URL of the NDES server and the challenge generated by Intune. A policy has already been pushed to the device by the Intune service. This policy contains the URL of the NDES server and the challenge generated by Intune.
- During the next sign-in, the user is prompted to configure Windows Hello for Business, confirm their identity using multifactor authentication, and create a PIN. A private key is created and registered in Azure AD. The user can also initiate the Windows Hello setup process from the Settings app at any time.
- The device contacts the internet-facing NDES server using the URL from the NDES server and provides the challenge response. The NDES server validates the challenge with the CRP and receives a “true” or “false” to challenge verification.
  - If the challenge response is “true,” the NDES server communicates with the certificate authority (CA) to get a certificate for the device. Appropriate ports need to be open between the NDES server and the CA for this to happen.
- The NDES server delivers the certificate to the computer.

Setting policies
CSEO used domain-based Group Policies to push out policy-based settings to configure our Windows 10 domain-joined devices to provision Windows Hello user credentials when users sign in to Windows. Non-domain joined devices receive their policies from Intune. We also used these settings to define the complexity and length of the PIN that our users generate at registration and to control whether Windows Hello was enabled.
We had the option to configure whether we would accept certificate-based Windows Hello for Business with PIN as a software-backed credential. We chose to enable Windows Hello for Business with a hardware-required option, which means that keys are generated on TPM 2.0.

**Policies for Active Directory domain-joined clients**
You must create and deploy a Group Policy object using the settings found under User Configuration > Administrative Templates > Windows Components Windows Hello for Business.

The Group Policy object contains the policy settings needed to trigger Windows Hello for Business provisioning and to ensure Windows Hello for Business authentication certificates are automatically renewed. Both the Enable Windows Hello for Business setting and the Use certificate for on-premises authentication setting must be enabled.

Windows 10 also provides PIN complexity settings for control over PIN creation and management. Beginning with Windows 10 version 1703, the policy settings are found under Computer Configuration > Administrative Templates System > PIN Complexity.

**Policies for Azure Active Directory-joined clients**
To use the Windows Hello/Windows Hello for Business certificate-based sign-in, configure the certificate profile (Assets & Compliance > Compliance Settings > Company Resource Access > Certificate Profiles). Select a template that has smart card sign-in extended key usage. Note that to set the minimum key size set, this certificate template should be configured in the Simple Certificate Enrollment Protocol (SCEP) Enrollment page—then you can use the Windows Hello for Business and Certificate Properties page to set the minimum key size set to 2048.

To set up the desired policy, we also need to create a new Windows Hello for Business profile (Assets & Compliance > Compliance Settings > Company Resource Access > Windows Hello for Business profiles) and specify the following required options:

- Use Windows Hello for Business
- Use a hardware security device
- Use biometrics
- PIN Complexity

**User enrollment experience**
When a domain-joined computer running Windows 10 Anniversary Update or later pulls Group Policy settings from a domain controller, certificate enrollment policies and the Windows Hello for Business policies are applied to the Windows 10 computer, provided all the criteria for policy application are met.

**Client signs out and signs in (and unlocks) the device**
The user unlocks their device, and the certificate enrollment process is triggered.

**Certificate enrollment process**
After a PIN is successfully created, the scheduled task runs (triggered by Event ID 300, which is “Key registration was successful.”). It checks for an existing certificate. If the user doesn’t have one, the task sends the requests for a new challenge.

At this point, Windows 10 calls on the specified Certificate Services server through AD FS and requests a challenge with an expiration time. If the PIN is cached, the certificate enrollment is triggered.

**Certificate renewal behavior**
We have configured PIN credential certificates to have a lifetime of 90 days from when they are issued. Renewals will happen approximately 30 days before they expire. When a user next enters their Windows Hello for Business PIN within the 30 days prior to its expiration, a new certificate will be automatically provisioned on their device.

Certificate renewal is governed by Group Policy settings for auto-enrollment. The system checks for certificate lifetime percentage and compares it against the renewal threshold. If it’s beyond the set threshold, a certificate renewal starts.
Microsoft Intune specifics
The Open Mobile Alliance Device Management client talks to the Microsoft Intune mobile device management server using SyncML. Policies are routed, and then the user receives the Simple Certificate Enrollment Protocol profile, as configured in our hybrid environment, deployed through Microsoft Intune. Within 10 minutes, the user should receive a certificate. If that fails, the user needs to manually sync.

Service management
We manage identity as a service at Microsoft and are responsible for deciding when to bring in new types of credentials and when to phase out others. When we were considering adding the Windows Hello for Business feature, we had to figure out how to introduce the new credential to our users, and to explain to them why they should use it. Windows Hello for Business isn’t replacing passwords at Microsoft, but it does allow our users to securely sign in to their device and provides them seamless access to both on-premises and cloud resources.

Driving adoption
Before the release of Windows 10 November update at Microsoft, it was rolled out to approximately 15,000 early adopters. These users validated the new credential functionality and user scenarios, and they provided valuable feedback that we shared with the product development team.

After the internal release of Windows 10 November update, we made it a requirement that users install the update on all domain-joined Windows 10 computers. Users were notified that they had three weeks in which they could voluntarily install the update and begin using the new credentials. Of the 189,000 compatible user devices at Microsoft, so far 111,000 of the devices are enrolled in Windows Hello for Business.

One of the main challenges for adoption is that the users have multiple options—including old credentials, like virtual smart cards—they have been using for the last few years. We’re addressing this in two ways: targeted user awareness and training on the benefits of using a PIN. This increased awareness, and training is resulting in increased use of a PIN as the sign-in method.

Measuring service health
We’re in the process of creating end-to-end telemetry to measure the service health of Windows Hello for Business. For now, we’re monitoring the performance and status of all our servers. We’re also expanding the service, so adoption and usage numbers are very important metrics that demonstrate the success of our service. We also track the number and types of help desk issues that we see.

We use custom reports created from certificate servers and custom telemetry service metrics to collect prerequisites, and key and certificate issuance times for troubleshooting. Detailed reports about other aspects of the service can also be generated from Microsoft Intune.

We configure a user’s certificate to expire, and certificate renewals are issued with the same key. When necessary, the certificates can be revoked directly though Microsoft Intune, which provides easier administration.

Lessons learned

TPM issues
OEM BIOS initialization instructions and TPM lockout policies are OEM-specific. We performed steps to identify and document the potential issues for each hardware provider. We also communicated to our users that clearing a TPM will cause their private key to not work in Windows Hello for Business.

Preventing PIN enrollment problems
Some of the common issues we saw with users creating their PINs could have been avoided with better communication. These issues include users not understanding the prerequisites, and not signing in and then signing out with their user name and password. To help avoid this issue, we created a productivity guide to walk users through the steps.

microsoft.com/itshowcase  January 2020
Limiting certificate issuance traffic
NDES is a single-threaded app. To effectively funnel high volumes of traffic from clients enabling their PINs on busy days, we have limited the concurrent connections to 300 per NDES server for optimum performance. When the number of connections exceeds the limit, users receive a "service is busy" error, instead of performing automatic retries that cause performance issues.

Monitoring end-to-end service health
Windows Hello for Business relies on several underlying services: Azure AD, AD FS, Microsoft Intune, NDES, and CA. All of these services need to be healthy and available. Certificate issuance delays can be hard to troubleshoot, but monitoring the health and performance of the supporting services can help.

For more information
Microsoft IT Showcase
microsoft.com/itsshowcase
Implementing a Zero Trust security model at Microsoft
Keeping Windows 10 devices up to date with Microsoft Intune and Windows Update for Business
Managing Windows 10 devices with Microsoft Intune
How Microsoft is modernizing device management

Active Directory and Azure Active Directory
Integrating your on-premises identities with Azure Active Directory
Connect domain-joined devices to Azure AD for Windows 10 experiences
Azure AD Join on Windows 10 devices

Management
Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS)
PART 2 - SCEP certificate enrolling using ConfigMgr 2012, CRP, NDES and Windows Intune

Policy Management
Using a Policy Module with the Network Device Enrollment Service

© 2020 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.